② حسب مبرهنة فإن x, y, z ثلاثية فيثاغورث أولية وتحقق الشروط

$d(r, s) = 1$ و

$x = r^2 - s^2$ ؛ $y = 2r.s$ ؛ $z = r^2 + s^2$

و r, s أحدهما زوجي والآخر فردي

أ) اذا كان $3 | y$ تم المطلوب

ب) اذا كان $3 \nmid y$ ؛ $3 \nmid 2r.s$ وبالتالي لا يمكن 3 أن تقسم r و s

$3 \nmid 2$ و $3 \nmid r$ ∧ $3 \nmid s$ (لأن r و s أوليان فيما بينهما)

معنى ذلك باقي r و s على 3 إما 1 أو 2

أي $r = 3q + 1$ ∧ $s = 3q_1 + 1$

$r = 3q + 2$ ∧ $s = 3q_1 + 2$

عندئذ

أ) $x = r^2 - s^2 = (3q+2)^2 - (3q_1+1)^2$

وبالتالي 3 تقسم x.

ب) $x = r^2 - s^2 = (3q+1)^2 - (3q_1+2)^2$

وبالتالي 3 تقسم x.

③ مركز الدائرة المماسة لأضلاع مثلث داخلاً هو نقطة تلاقي المنصفات

مركز الدائرة المارة برؤوس المثلث هي نقطة تلاقي المتوسطات

لنفرض أن x و y ضلعين في المثلث القائم و z الوتر

R نصف قطر الدائرة المماسة لأضلاع المثلث

وبالتالي مساحة المثلث

$S = \frac{1}{2} x.y = \frac{1}{2} R (x+y+z)$

/ /

ولكن كان (x,y,z) ثلاثي فيثاغورث أولي وبالتالي حسب مبرهنة

$$\begin{cases} x = r^2 - s^2 & \Rightarrow x = k(r^2 - s^2) \\ y = 2r.s & \Rightarrow y = k(2r.s) \\ z = r^2 + s^2 & \Rightarrow z = k(r^2 + s^2) \end{cases}$$

$$R = \frac{x.y}{x+y+z} = \frac{k^2.2.r.s(r^2-s^2)}{k(r^2-s^2+2r.s+r^2+s^2)} \quad \rightarrow (r+s)(r-s)$$

$$= ________ = k.s(r-s)$$

وبالتالي R عدد صحيح ($\because$ لأن k عدد صحيح و s عدد صحيح و $(r-s)$ عدد صحيح) وبالتالي جداء أعداد صحيحة عدد صحيح

التطابقات

تعريف:

ليكن العدد $m \in \mathbb{Z}^+$ وليكن $a, b \in \mathbb{Z}$ نقول إن a يطابق b بالمقياس m إذا كان لهما نفس الباقي عند تقسيمهما على m أي إذا كان $m \mid (a-b)$

ونكتب رمزياً:

$$a \equiv b \pmod{m}$$

وإلا نقول a لا يطابق b بالمقياس m.

صفوف البواقي:

. نعلم أن عند تقسيم أي عدد صحيح n على m يكون

$n = q \cdot m + r$, $0 \le r < m$, $m > 1$

أي $r \in \{0, 1, 2, \dots, m-1\}$

وبالتالي تتجزأ $\mathbb{Z}$ إلى m مجموعة جزئية وبالتالي كل أي عدد صحيح سينتمي إلى إحدى هذه المجموعات

وهذه المجموعات تشكل تجزئة لـ $\mathbb{Z}$:

أ) اتحادها هو $\mathbb{Z}$

ب) تقاطع أي اثنين منها هو ϕ.

ج) أي منها لا يساوي ϕ

و r أي عدد من أي صف

$\bar{2} = \{mt + 2 : t \in \mathbb{Z}\}$

ويمكن اعتبار أي عدد صحيح من هذا الصف ممثلاً له.

ليكن $m = 6$

$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \cup \bar{4} \cup \bar{5}$

لدينا المجموعة

$\{0, 1, 2, 3, 4, 5\}$ مجموعة ممثلات الصفوف التكافؤ

$\{6, 7, 8, 9, 10, 11\}$ هذه المجموعة تختلف عن المجموعة السابقة فقط بالشكل

وبالتالي هذه المجموعة أيضاً تمثل مجموعة ممثلات الصفوف التكافؤ



وبالتالي تسمى المجموعة $\{0,1,2,3,4,5\}$
مجموعة البواقي التامة الصغرى المفضلة

ملاحظة:

1- من تعريف التطابق ينتج انه اذا كان $a \equiv b \pmod m$
فانه a و b ينتميان إلى صف واحد من صفوف البواقي بالمقياس m
اذا كان $a \not\equiv b \pmod m$
وهذا يعني أن a و b يقعان في صفين مختلفين بالمقياس m

2- إن أي عدد صحيح n يطابق باقي قسمته على العدد m
لأن $n = q \cdot m + r$
حيث r يحقق الشرط وبالتالي
$\Leftarrow$ $n - r = q \cdot m$
وبالتالي $m \mid (n-r)$ $\Leftarrow$
$n \equiv r \pmod m$

الخواص العامة للتطابقات:

$a \equiv b \pmod m$ $\Leftrightarrow$ $m \mid (a-b)$

نفرض أن $a, b, c, d \ldots \in \mathbb{Z}$

1- إن علاقة التطابق هي علاقة تكافؤ تحقق الشروط

أ- انعكاسية $\forall x \in \mathbb{Z} \mid x \equiv x \pmod m$

ب- تناظرية $x \equiv y \pmod m \Rightarrow x \equiv y \pmod m$

ج- متعدية

$x \equiv y \pmod m \wedge y \equiv z \pmod m$
$\Rightarrow x \equiv z \pmod m$

2- إذا كان $a \equiv b \pmod m$ $\Rightarrow$ $ka \equiv kb \pmod m$
$\forall k \in \mathbb{Z}$

بما أن $m \mid (a-b)$ وبالتالي تقسم مضاعفات $(a-b)$ أي $k(a-b)$

أي $m \mid k(a-b)$ وبالتالي

$m \mid ka - kb$

أي $ka \equiv kb \pmod{m}$

3- إذا كان $a \equiv b \pmod{m}$ و $c \equiv d \pmod{m}$ وبالتالي

$$a \pm c \equiv b \pm d \pmod{m}$$

ممكن تقسيم الجمع في كل جهة والجمع لا يهتز الاتزان الرياضي

وكذلك

$$a \cdot c \equiv b \cdot d \pmod{m}$$

4- إذا $a \equiv b \pmod{m}$ فإن $a^n \equiv b^n \pmod{m}$

حيث n عدد صحيح موجب

من صفة التجزئة

5- إذا كان $a \equiv b \pmod{m}$ وكان $f(x) = \sum_{i=0}^{n} c_i x^i$ (كثيرة حدود) حيث $c_i \in \mathbb{Z}$ وبالتالي

$$f(a) \equiv f(b) \pmod{m}$$

مثال

$$2 \equiv -4 \pmod{6}$$

$2 = 0 \cdot 6 + 2$

$-4 = (-1) \cdot 6 + 2$

} a و b لهما نفس باقي القسمة على 6

أو $6 \mid 2-(-4) = 2+4 = 6$ (6 تقسم نفسها)

وليكن $f(x) = x^2 - x + 10$

$f(2) = 4 - 2 + 10 = 12$

$f(-4) = 16 + 4 + 10 = 30$

مثال:

$$12 \equiv 30 \pmod 6$$

$$6 \mid (12-30) = -18$$

6- اذا كان

$$ka \equiv kb \pmod m$$

فإن

$$a \equiv b \pmod{\frac{m}{d}}$$

حيث $d = d(m, k)$

ملاحظة: لو كان k أولي مع m أي $d(m,k) = 1$ فعندئذ

$$ka \equiv kb \pmod m$$

$$\Rightarrow a \equiv b \pmod m$$

يمكن الاستخدام العامل المشترك من طرفي التطابق اذا كان هذا العامل أوليًا مع المقياس

7- إذا كان $ka \equiv kb \pmod p$ حيث p عدد أولي لا يقسم k فعندئذ

$$a \equiv b \pmod p$$

8- اذا كان $a \equiv b \pmod m$ و n قاسم لـ m ($n \mid m$)

فعندئذ

$$a \equiv b \pmod n$$

لأن $m \mid (a-b)$ ، $n \mid m$ وبالتالي $n \mid (a-b)$ اي

$$a \equiv b \pmod n$$

9- إذا كان $a, b \in \mathbb{Z}$ و $m_i \in \mathbb{Z}^+$ ، ($i = 1, 2, \ldots, k$)

وكان

$$a \equiv b \pmod{m_i}$$

$$\Leftrightarrow$$

$$a \equiv b \pmod{\operatorname{lcm}(m_1, m_2, \ldots, m_k)}$$

أو $a \equiv b \pmod m \; ; \; m = \operatorname{lcm}(m_1, m_2, \ldots, m_k)$

بالتالي m_i تقسم m

ملاحظة: اذا كان $m_1, m_2, \ldots, m_k$ أولية نسبياً فيما بينها مثنى مثنى فإنه

$$a \equiv b \pmod{m_1 \cdot m_2 \cdots m_k}$$

-10 اذا كان $a \equiv b \pmod{p^r}$ حيث p عدد أولي و $r \geq 1$ فإنه

$$a^{p^s} \equiv b^{p^s} \pmod{p^{r+s}}$$ و $s \geq 0$

نبرهن بالاستقراء الرياضي.

مثال:

$$a \equiv b \pmod{2^3}$$
$$\Rightarrow a^{2^5} \equiv b^{2^5} \pmod{2^{3+5}}$$

بالاستقراء على s , $s \geq 0$ من أجل $s=0$

$$a^{p^0} \equiv b^{p^0} \pmod{p^{r+0}} \Rightarrow a \equiv b \pmod{p^r}$$

العلاقة صحيحة من أجل $s=0$

نفرض صحتها من أجل $s=k$ ولنثبت صحتها من أجل $s=k+1$

$$a^{p^k} \equiv b^{p^k} \pmod{p^{r+k}}$$

هذا يعني أن

$$p^{r+k} \mid (a^{p^k} - b^{p^k}) \Rightarrow (a^{p^k} - b^{p^k}) = M \cdot p^{r+k} \quad , M \in \mathbb{Z}$$

$$a^{p^k} = M \cdot p^{r+k} + b^{p^k}$$

نرفع طرفي المساواة للأس p

$$(a^{p^k})^p = (M \cdot p^{r+k} + b^{p^k})^p \rightarrow$$

$$\downarrow$$
$$a^{p^{k+1}}$$

حسب ثنائي حد نيوتن نجد

/ /

بدءاً من الحد الثاني $r+k+1$ ، $2r+2k+1$ ، ---- وجميعها أكبر من $r+k+1$

.. جميع الحدود بدءاً من الحد الثاني تقبل القسمة على p^{r+k+1}

وهذا يعني أن $a^{p^{k+1}}$ تطابق $b^{p^{k+1}}$ أي

$$a^{p^{k+1}} \equiv b^{p^{k+1}} \pmod{p^{r+k+1}}$$

تمرين: أثبت أن الفرق بين أي عدد صحيح n بالنظام العشري ومجموع أرقامه يقبل القسمة على 9.

أي يقبل عدد ما القسمة على 9 إذا وفقط إذا قبل مجموع أرقامه القسمة على 9.

إن أي عدد بالنظام العشري N يكتب على النحو:

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 10 + a_0 = (a_n, a_{n-1}, \cdots, a_0)$$

وحيث أن $10 \equiv 1 \pmod 9$ وبالتالي

$$(10)^2 \equiv 1^2 \pmod 9$$

$$\vdots$$

ومنه: $(10)^k \equiv 1 \pmod 9$

$$N \equiv (a_n + a_{n-1} + \cdots + a_1 + a_0) \pmod 9$$

هذا يعني أن:

$$9 \mid (N - \sum_{i=1}^{n} a_i)$$

يقبل عدد القسمة على 9 إذا وفقط إذا قبل مجموع أرقامه القسمة على 9

تمرين: سؤال امتحان

أثبت أن من أجل أي عدد صحيح موجب n يكون $15 \mid (2^{4n} - 1)$

أو (بين أن)

بين أن 2^{4n} يقبل القسمة على 15 أم لا ؟ ولا يقبل القسمة لأن باقي قسمته على 15 لا يساوي 1

$$2^{4n} = (2^4)^n$$

لأن 2^4 يساوي 16 وهنا نطابقه

$$2^4 \equiv 16 \equiv 1 \pmod{15}$$

$$(2^4)^n \equiv 1 \pmod{15}$$

باقي القسمة يساوي صفر

$$2^{4n} \equiv 1 \pmod{15} \Rightarrow 15 \mid (2^{4n} - 1)$$

تمرين 3 -

1 - بين إن كان العدد $3^{2n} + 7$ يقبل القسمة على 8 أم لا

$$3^{2n} \equiv 1 \pmod 8$$

نضيف 7 إلى طرفي التطابق

$$3^{2n} + 7 \equiv (7+1) \pmod 8$$

وبالتالي

$$3^{2n} + 7 \equiv 0 \pmod 8$$

وبالتالي.

$$8 \mid (3^{2n} + 7)$$

أوجد أصغر عدد صحيح موجب K يحقق العلاقة

$$31 \mid [(33)(26)^2 - K]$$

العدد المطلوب K هو باقي قسمة $(33)(26)^2$ على 31

أي أوجد باقي القسمة

$$(33)(26)^2 \overset{?}{\equiv} K \pmod{31}$$

نلاحظ.

$$33 \equiv 2 \pmod{31}$$

$$26 \equiv -5 \pmod{31}$$

إذا أخذنا.

$$Z_{31}$$

نظير
$(\overline{26}) + (\overline{\quad}) = \overline{31} = \overline{0}$

$-(\overline{26}) = 5$

$(\overline{26}) = -5$

وبالتالي نظير 26 هو 5 - علينا التعامل مع 5- بدلاً من 26 أي

$(26)^2 \equiv 25 \pmod{31}$

$(33)(26)^2 \equiv 50 \pmod{31}$

$\equiv 19 \pmod{31}$

وبالتالي $K = 19$

تمرين:

أوجد باقي قسمة $\sum_{1}^{1000} k!$ على 24 .

$\sum_{1}^{1000} k! = 1! + 2! + 3! + 4! + \text{-----}$

$= 1 + 2 + 6 + \underline{24} + 5! + \text{---}$

باقي القسمة على 24 يساوي الصفر

باقي قسمته على 24 يساوي الصفر

بدءاً من الحد الرابع من هذا المجموع جميع الحدود تقبل القسمة على 24 بلغة التطابق

هي تطابق الصفر بالمقاس 24 وبالتالي

$\sum_{1}^{1000} k! \equiv (1+2+6) \pmod{24}$

أي تطابق 9 .

أي باقي قسمة $\sum_{1}^{1000} k!$ على 24 هو 9 .

تمرين:

بين أن مهما كان أي عدد صحيح a يكون

$a^2 \equiv 0 \text{ or } 1 \text{ or } 4 \pmod 8$

/ /

إذا كان a فردي باقي قسمته على 8 هو 1

إذا كان a زوجي فإنه من الشكل $a = 2q$ وبالتالي $a^2 = 4q^2$

وبالتالي q يمكن أن تكون زوجية أو تكون فردية.

إذا كان لدينا عدد باقي قسمته على 8 هو 0 أو 1 أو 4 (مربعه)

وبالتالي لا يمكن أن يكون مربعاً كاملاً

اختبارات هامة لقابلية القسمة:

- عينية:

① إن $(10)^n$

$$(10)^n \equiv 0 \pmod{2^k}$$

لكل عدد صحيح موجب $n \geq k$ وكذلك

②:

$$(10)^n = 0 \pmod{5^k}$$

الإثبات: ① و ②

إن $10 = 2 \cdot 5$ ومنه

$(10)^k = 2^k \cdot 5^k$ فقط في كلمات التبديلية

أي أن:

$$2^k \mid 10^k \quad \wedge \quad 5^k \mid 10^k$$

⇐

$$2^k \mid 10^n \quad ; n \geq k$$

$$\wedge$$

$$5^k \mid 10^n \quad ; n \geq k$$

وبذلك يتم المطلوب.

برهنة: نفرض أن التمثيل العشري للعدد N من الشكل،

$$N = (a_m a_{m-1} --- a_1 a_0)_{10} \quad ; \quad 0 \leq a_k \leq 10$$

a_k عدد صحيح.

ولنفرض $T = \sum_{k=0}^{m} (-1)^k a_k$ و $S = \sum_{k=0}^{m} a_k$

ولكن

$$N_k = (a_{k-1} --- a_1 a_0)$$

عندئذ يكون،

① $2^k | N$ إذا وفقط إذا كان $2^k | N_k$

$k=1$ $N_k = (a_0)$ مرتبة واحدة

يقبل القسمة عدد ما على 2 إذا وفقط إذا قبل آحاده القسمة على 2.

$k=2$:

$2^2 = 4$: $N_2 = (a_0, a_1)$

يقبل القسمة عدد ما على 4 إذا وفقط إذا قبل آحاده وعشراته على 4.

$k=3$:

$2^3 = 8$ $N_3 (a_0, a_1, a_2)$

يقبل عدد ما القسمة على 8 إذا وفقط إذا قبل آحاده وعشراته ومئاته القسمة على 8.

② $5^k | N$ إذا وفقط إذا كان $5^k | N_k$

يقبل القسمة عدد ما على 5 إذا وفقط إذا كان آحاده صفر أو 5.

③ $3 | N \Leftrightarrow 3 | S$

يقبل القسمة على 3 إذا وفقط إذا كان مجموع أرقامه يقبل القسمة على 3

④ $9 | N \Leftrightarrow 9 | S$

⑤ $11 | N \Leftrightarrow 11 | T$

مبرهنة:

إذا كان $n = (1000)\, q(n) + r(n)$

وكان العدد $c = 7 \text{ or } 11 \text{ or } 13$ فإن

$c \mid n \iff c \mid [q(n) - r(n)]$

ملاحظة:

$7 \cdot 11 \cdot 13 = 1001$

$q(n) - r(n) = q(n) - [n - 1000\, q(n)]$

$= 1001\, q(n) - n$

وبالتالي 7 تقسم 1001 و 13 أيضاً و 11.

$$q(n) - r(n) = 1001\, q(n) - n$$

فإن الشرط اللازم الكافي لكي تقسم أحد الأعداد n يجب أن تقسم الطرف الأيسر أي

$q(n) - r(n)$.